A New Class of Burst-Correcting Cyclic Codes

B. Arazi[1]
Communications Systems Research Section

In many DSN communication systems (the GCF, computer-computer data transfer, etc.) transmission errors tend to occur in intermittent bursts. In this article a new class of burst-error-correcting codes, potentially applicable to DSN systems, is described. Many of these codes are superior to any previously known.

I. Introduction

A systematic way of constructing burst-correcting cyclic codes is presented. If the length of the burst and the length of the codeword are denoted by b and n, respectively, then for $b \geq 30$ and $b/n \leq 5$ percent, these codes outperform the most efficient burst-correcting codes known, in most cases. (For the same b and n, the rate of the suggested code is higher.)

The main advantage of the suggested code lies in the simple hardware implementation of both encoder and decoder. The encoder uses a feedback shift register with a simple structure of feedback connections. The decoder uses only two end-around shift registers.

II. Presentation

Theorem

(1) Let q be a prime and let $q > p$, where p is a positive integer. The polynomial $g(X) = (X^q + 1)(X^p + 1)/(X + 1)$ generates a cyclic code. The length of a codeword is $q \cdot p$.

(2) The code is capable of correcting any error burst of length $p - 1$ or less iff $p - n(q-p)$ is prime for $n = 0,1,2, \cdots, [p/(q-p)]$.

(3) Let b denote the length of an error burst.

(a) If $b \leq \max(p + 1, q - p + 1)$ the error is detected.

[1]Visiting from the National Electrical Engineering Research Institute, South Africa.

(b) If $\max(p + 1, q - p + 1) < b < q$ then the probability of not detecting an error is less than $p \cdot 2^{p-q-1}$.

The proof is given in the Appendix.

Table 1 shows some cases where such a code can be used. (The efficiency is defined as $(2b + 2)/(n - k)$. The numerator is the minimum theoretical number of parity bits needed for correcting a burst of length b or less and detecting all bursts of length $b + 1$ and $b + 2$. The denominator is the actual number of parity bits used. The efficiency is an important feature of a code. (If a shortened version of the code is used, the higher the efficiency the higher the rate is.) These codes are suitable for correcting long bursts inside relatively long codewords. (If $t \leq b < u - 1$, where t and u are two successive primes, that code is selected which corrects a burst of length $u - 1$ or less.)

For those cases where $b \geq 30$ and $b/n \leq 5$ percent, these codes outperform the known codes in most of the cases (higher rate and higher efficiency). A list of the known codes is given in Ref. 1. "These codes and the codes derived from them by interlacing (interleaving) are the most efficient single burst error correcting codes known."

Table 2 compares the performance of the suggested code and the known codes for the same values of b and n. (In order to achieve the specified values of b and n, the known codes were interleaved. Both codes were shortened when necessary. Table 2 demonstrates how, in most cases, the suggested code outperforms slightly the most efficient codes known. Its main importance lies, however, in the simplicity of the hardware implementation of both encoder and decoder.

The encoder of a cyclic code consists of a shift register and a feedback loop to which some stages are connected (via an exclusive OR gate), according to the coefficients of the generator polynomial. In our case,

$$\begin{aligned} g(X) &= (X^q + 1)(X^p + 1)/(X + 1) \\ &= (X^q + 1)(X^{p-1} + X^{p-2} + \cdots + 1) \\ &= X^{q+p-1} + X^{q+p-2} + \cdots + X^q \\ &\quad + X^{p-1} + X^{p-2} + \cdots + 1 \end{aligned}$$

It follows that the encoder consists of a shift register with $q + p - 1$ stages from which the first and last $p - 1$ stages are all connected to the feedback loop.

After considering the structure of the parity check matrix H given in the proof of the theorem, it follows that the decoding operation which is performed by multiplying H by the received message, can have a simple form, which is shown in Fig. 1.

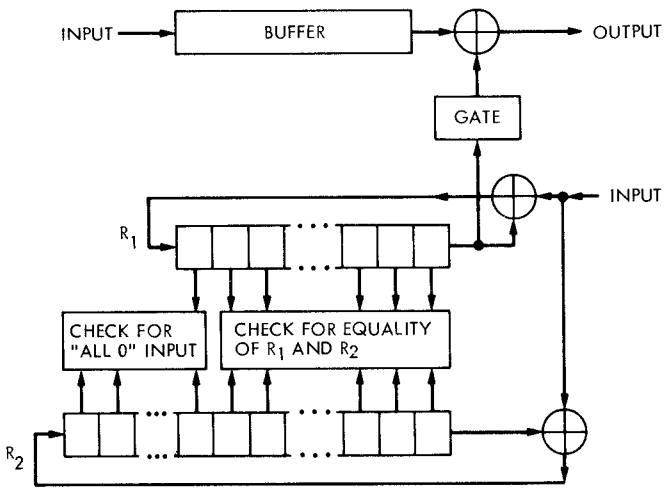


Fig. 1. The decoder

The received message is shifted into a buffer, and also into registers R_1 and R_2, which are a p-stage and a q-stage register, respectively. After the complete message has been received, a check is made to determine whether the content of the registers is "all 0." If this is the case, no error has been detected and the received message is shifted out of the buffer without any correction.

If an error is detected, the content of the last stage of R_1 (counting from the right), as well as the last $(q - p + 1)$ stages of R_2 are checked as to being "all 0." At the same time the contents of the ith stages of R_1 and R_2, $1 \leq i \leq p - 1$, are checked for being identical. If either one of the two checks described fails, the bits stored in the buffer are shifted out one at a time, while the gate is closed. For each bit leaving the buffer, both registers are shifted cyclically by one place (the input is constantly logic 0) and the checks described are performed for each shift.

When both checks have been satisfied (one check shows "all 0" input and the other shows identity of the content of the first $p - 1$ stages) the gate is opened and the content of R_1 is added bit by bit to the bits shifted out of the buffer and the correction is completed.

The advantage of the described decoder lies in the fact that it does not use feedback connections at all. On the

other hand, when implementing the decoder of the known cyclic codes, some complicated feedback connections are made according to the coefficients of the generator polynomial.

The theorem considers also the case where $q - p + 1 > p + 1$, which means that $q > 2p$. Notice that if p and q are primes where $q > 2p$ it follows from the theorem that the code generated by $(X^p + 1)(X^q + 1)/(X + 1)$ is capable of correcting any error burst of a length $p - 1$ or less.

Clarifying the concept of error detection is also worthwhile. An error is detected when the decoder detects the existence of an error, together with the fact that it is uncorrectable, such that no false attempt is made to correct the error. Referring to the described decoder, an error is detected when either one of the two checks performed is not satisfied by the time the message is shifted completely out of the buffer.

The following demonstrates the ability of the code for the case where $p = 31$ and $q = 101$:

(1) Any error burst of length 30 or less is corrected.

(2) Any error burst of length 71 or less is detected.

(3) The probability of not detecting an error of a length between 72 and 100 is less than 10^{-20}.

(4) By keeping $p = 31$ and changing q, it is possible to achieve almost any desirable error detection capability.

The theorem states that the condition posed on the values of p and q is also a necessary condition. It is worthwhile demonstrating why it is not enough to require that p and q should be prime.

Let X be a set of positive integers which are the locations of the erroneous bits inside the received message. Let A and B be the sets of residues of the elements of X modulo p and q, respectively. It follows from the structure of the decoder that by the time the received message is stored completely in the buffer, the locations of the 1 elements in R_1 and R_2 are the elements of A and B, respectively.

An error burst cannot be corrected uniquely if a set Y, which is different from X, produces the same residue sets A and B. Two such sets X and Y can exist although p and q are primes. For example: $p = 11$, $q = 13$.

$$X = \{11,12,14,15,19,20\}, \quad Y = \{58,59,63,64,66,67\}$$
$$A = \{1,3,4,8,9,11\}, \quad B = \{1,2,6,7,11,12\}$$

The elements in both X and Y are confined to 10 successive places since the error burst is of length $p - 1$ or less.

Reference

1. Lin, S., *Introduction to Error Correcting Codes*, Prentice-Hall, Inc., Englewood Cliffs, N.J., 1970.

Appendix

Proof of the Theorem

Step 1: Proof of part (1) of the theorem

The greatest common divisor of $X^p + 1$ and $x^q + 1$ is $X^{(q,p)} + 1 = X + 1$. Since $X^p + 1$ and $X^q + 1$ are both divisors of $X^{q \cdot p} + 1$, the polynomial $g(X) = (X^p + 1)(X^q + 1)/(X + 1)$ is also a divisor of $X^{q \cdot p} + 1$, which is a necessary and sufficient condition for $g(X)$ to generate a cyclic code of length $p \cdot q$.

Step 2: Finding a parity check matrix

Let us define a polynomial $h(X)$,

$$h(X) = (X^{q \cdot p} + 1)/g(X)$$

$$= [(X^{p \cdot q} + 1)(X + 1)]/[(X^p + 1)(X^q + 1)].$$

The rows of the parity check matrix H consist of multiples of $h(X)$ (a polynomial is regarded as the row of a matrix when its coefficients form the elements of the row). In our case, $p + q - 1$ rows should be linearly independent. (Usually the number of rows of a parity check matrix equals the number of independent parity checks. However, if some extra rows which are a linear combination of the independent ones are added, the obtained matrix is still a parity check matrix in the sense that a syndrome **S** is defined as $H\,\mathbf{X} = \mathbf{S}$ where **X** is the received message. The syndrome **S** is the "all 0" vector iff **X** is a transmitted codeword.)

Let $m_i(X) = h(X) \cdot X^i \cdot (X^q + 1)/(X + 1) = X^i(X^{q \cdot p} + 1)/(X^p + 1) = X^i(X^{(q-1)p} + X^{(q-2)p} + \cdots + X^p + 1)$ $i = 0,1, \cdots, p - 1$.

$s_i(X) = h(X) \cdot X^i(X^p + 1)/(X + 1) = X^i(X^{q \cdot p} + 1)/(X^q + 1) = X^i(X^{(p-1)q} + X^{(p-2)q} + \cdots + X^q + 1)$ $i = 0,1, \cdots, q - 1$.

Let the first p rows of a matrix H consist of the polynomials $m_i(X)$ and let its last q rows consist of the polynomials $s_i(X)$. This matrix can be described in a very simple way. Its first p rows consist of the unity matrix of order $p \times p$ written successively q times. A similar description applies for the last q rows.

For example, for $p = 2, q = 3$,

$$H = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

The sum of the rows of H is the "all 0" vector, which means that any particular row equals the sum of all the other rows. In view of the structure of H it is obvious that if one row is omitted, the rest $q + p - 1$ rows are linearly independent and H is therefore a parity check matrix of the code.

Step 3: Analyzing the syndrome

Let **X** be a codeword generated by $g(X)$ and let $\mathbf{Y} = \mathbf{X} + \mathbf{N}$ be the received message where **N** is an error burst of length $p - 1$ or less. Let E be a vector of length $p - 1$ whose elements are the error pattern, where its first element is 1. (If the burst is of length $d < p - 1$, the last $p - 1 - d$ elements of E are 0). Let E_1 and E_2 be two binary vectors of length p and q respectively. The first $p - 1$ bits of both vectors equal the vector E, and the rest of their elements are 0.

Let $E_1^{(j)}$ and $E_2^{(j)}$ denote the vectors obtained from E_1 and E_2 by shifting them cyclically for j places. If the first erroneous bit of the error burst is in the jth place of the received message, then in view of the construction of H, the first p bits of the syndrome are the vector $E_1^{(j)}$ and its last q bits are the vector $E_2^{(j)}$. The error burst cannot be corrected iff there exists an error burst pattern F which starts at the kth place of the received message and which produces the same syndrome, where $F \neq E$ or $j \neq k$ (or both).

3.1 $F \neq E, j = k$. Such a case is impossible. (Two different error patterns which occur at the same place in the received message cannot produce the same syndrome.)

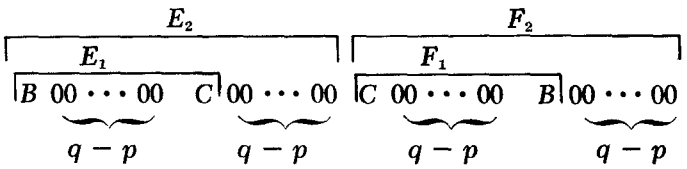
3.2 $F = E, j \neq k$. Since the same syndrome is produced it follows that $E_1^{(j)} = E_1^{(k)}$ and $E_2^{(j)} = E_2^{(k)}$. A vector can equal a cyclic shift of itself if all its elements equal each other. Such a case is impossible here since both E_1 and E_2 start with a 1 and end with a 0. Since the length of E_2 is prime, the last two equalities are possible iff $j - k$ is divisible by $r \cdot q$, where r is a divisor of p. (Generally, r can also be a product of p, but this is impossible here since $0 < j, k \leq p \cdot q$.) It follows that p must be factorized.

3.3 $F = E, j \neq k$. The theorem deals with error bursts of length $p - 1$ or less. The length of F is therefore $p - 1$ where F starts with a 1. (If the length of the burst whose pattern is represented by F is less than $p - 1$, the last elements of F are 0.) Let F_1 and F_2 be binary vectors of length p and q, respectively, both equal in their first $p - 1$ places to the vector F. The rest of their elements are 0. Since the same syndrome is produced by E and F it follows that $E_1^{(j)} = F_1^{(k)}$ and $E_2^{(j)} = F_2^{(k)}$.

Let $i \equiv j - k \pmod{p}$ and $m \equiv j - k \pmod{q}$. It follows that $F_1 = E_1^{(i)}$ and $F_2 = E_2^{(m)}$. If either $i = 0$ or $m = 0$ it will follow that $E = F$. Such a case was treated above. The rest of the proof will show that it is possible to have $F_1 = E_1^{(i)}$ and $F_2 = E_2^{(m)}$ where $i, m > 0$ iff $p - n(q - p)$ is factorized for some n.

The vectors E_2 and F_2 both start with a 1 and have $q - p + 1$ zeroes at the end. In order for F_2 to be obtained from E_2 by a cyclic shift, E_2 must have somewhere in it $q - p + 1$ successive zeroes (which are transferred to its end by the cyclic shift that produces F_2). These zeroes are followed by a 1 (which is transferred to the beginning of F_2) and therefore cannot be part of the last $q - p + 1$ zeroes at the end of E_2. It follows that E_2 has in it $q - p + 1$ successive zeroes confined to the first p places, which means that E_1 contains $q - p + 1$ successive zeroes.

The vectors E_1, E_2, F_1 and F_2 have therefore the following form.



where B and C are two vectors starting with a 1 and ending with a 0.

Step 4: A general description of the proof

Let D denote an "all 0" vector of length $s = q - p$. Let the length of the vectors B and C obtained in the previous step be denoted by r and t, respectively.

Assuming that $F_1 = E_1^{(i)}$, steps 5 through 11 of the proof analyze the value of p for all possible positive values of i. The various values of i are related to r, s and t.

It is shown that for each relation among i,r,s and t a certain vector V_i has two different structures which can exist simultaneously iff $p - n \cdot s$ is factorized for some n.

Figure A-1 describes how each step of the proof follows from the previous one. (The number near each branch refers to the corresponding step.) Consulting this drawing might simplify the reading of the proof.

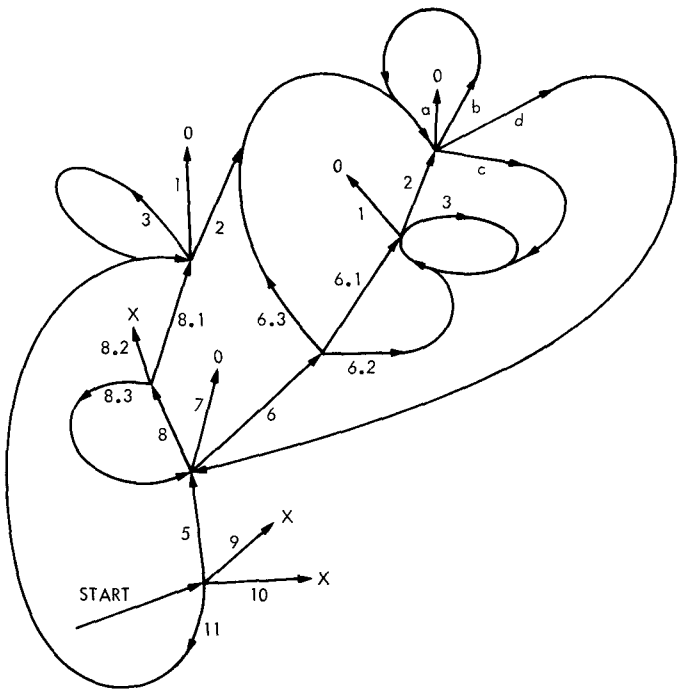


Fig. A-1. Description of the proof

The vector treated at the starting point is F_1. A last branch in a path (which is terminated by 0 or X for reasons explained later) corresponds to the structure of a certain vector V_i, and the path which starts with the starting point and ends with that last branch, shows the way by which V_i is obtained from F_1.

The vector whose structure corresponds to a last branch in a path is denoted by V_i if the path which connects the starting point to that branch connects on its way i branches to branches with a lower index. This excludes the case where step 11 continues with step 8.1. (If this connection is the only backwards connection in the path, the vector treated in the last branch is still V_0.)

When a branch is terminated with an X it means that a contradiction is met and the vector V_i, whose structure corresponds to this branch, cannot exist.

If a branch ending with a 0 corresponds to the structure of a vector V_0 whose length is d_0, it is proved that $d_0 - m \cdot s$ is factorized for some m.

When a branch in Fig. A-1 is connected to a branch with a lower index, it means that the proof arrives at an intermediate vector V whose structure is identical to that

of a vector V' treated previously, and the proof should therefore follow the same lines from that step on. (Within the proof, this reference to a previous step is of the form "continue with Eq. X." The equation preceding such a statement and Eq. X, are of the same form.)

Conclusion 1. It is enough to prove that $d_0 - m \cdot s$ is factorized for all possible V_0 in order to prove that $d_i - m \cdot s$ is factorized for all possible V_i (m does not have the same value for all V_0, but it is always some integer).

The factorization of $d_i - m \cdot s$ is in the sense that V_i consists of a set of subvectors. Of these subvectors m subvectors equal the vector D and the rest equal a vector A whose length is at least 2.

While reading the proof and observing the way by which the possible vectors V_1 are obtained (a vector V_1 is obtained when there is only one branch in the path which generates V_1 which is connected to a branch with a lower index), it is important to notice that if V_1 consists of subvectors which are either D or A, so does the vector V_0, which corresponds to the same last branch as V_1. This means that if $d_1 - m \cdot s$ is factorized, so is $d_0 - n \cdot s$, where m and n are positive integers.

The last statement can be extended by induction in the sense that V_{i+1} and V_1 can be treated as V_1 and V_0, respectively. It should also be noticed that $d_0 = p$.

Conclusion 2. If $d_i - m \cdot s$ is factorized for some V_i, so is $p - n \cdot s$.

Conclusion 3 follows from conclusions 1 and 2.

Conclusion 3. It is enough to prove that $d_0 - m \cdot s$ is factorized for all possible V_0, in order to prove that $p - n \cdot s$ is factorized for every possible structure of F_1 (assuming that $F_1 = E_1^{(i)}$ for $p > i > 0$).

Within the proof, the 4 different vectors V_0 are referred to as F_1 (since V_0 is the same vector treated at the starting point). However, in view of conclusion 3 it is enough to prove that $p - m \cdot s$ is factorized for those 4 vectors F_1 ($p = d_0$) in order to prove that $p - n \cdot s$ is factorized for all possible vectors F_1, where m and n are some integers.

Remark: In view of Fig. A-1, it might appear as if there are cases where a path enters an infinite loop and a terminating point is never reached. However, each time the path goes back to a step with a lower index, a shorter vector is treated. Since F_1 (which is the original vector treated) has a finite length, it is impossible to have an infinite loop.

(The case where step 11 continues with step 8.1 leaves the length of the vector unchanged. However, such a case can happen in one path only once.)

Notation: Throughout the proof, an equation of the type $X = HIJ$ means that a vector X consists of the vectors H, I, and J written successively. For example,

$$H = (abc),\ I = (de),\ J = (fgh),\ X = (abcdefgh)$$

Using this notation, $E_1 = BDC$ and $F_1 = CDB$.

Step 5: Assume $F_1 = E_1^{(i)}$, $0 < i < t$

$E_1 = BDC_1C_2$ where the length of C_2 is i.

$F_1 = C_2BDC_1$, but $F_1 = C_1C_2DB$. It follows that

$$C_2BDC_1 = C_1C_2DB \qquad \text{(A-1)}$$

where B, C_1, and C_2 all start with a 1 and end with a 0. (This statement follows from the fact that each one of the three vectors either starts or terminates E_1 or F_1.)

Let the length of C_1 be denoted by $u (u = t - i)$.

Step 6: Assume $F_1 = E_1^{(i)}$, $0 < i < t$, $u < r$

6.1 $i > u$

The two arrangements of F_1 shown in Eq. (A-1) can be described by the following drawing (Fig. A-2):

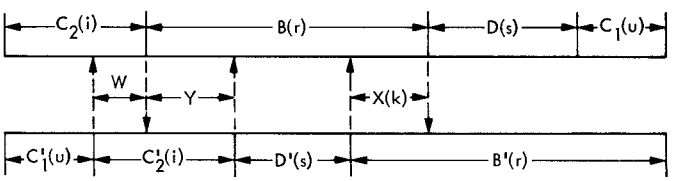


Fig. A-2. The two arrangements of F_1

The figures in the brackets denote the length of each vector. The vectors in the bottom drawing are denoted by "," although they are identical to the corresponding ones in the upper drawing. According to the drawing it appears that $r > s+u$. This must be the case since it is assumed that $r > u$. The vector B' starts with a 1 which must fall outside D (which is the "all 0" vector). A vector X whose length is $k = r - (s+u)$ *is* therefore obtained.

The following two equations follow from the drawing

$$B' = XDC_1$$

$$B = YD'X$$

It follows that

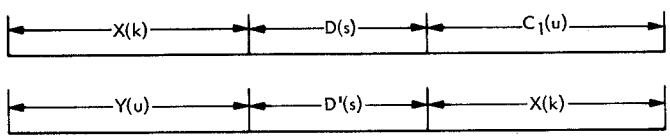
$$XDC_1 = YDX. \qquad \text{(A-2)}$$

Three different cases should be observed. These cases are: (1) $k < u + s$ and $u < k + s$. (2) $u > k + s$. (3) $k > u + s$. Any other relation among k, u and s involves an immediate correspondence between the first element of X or C_1 and an element in D, which is impossible since X and C_1 start with a 1, and D is the "all 0" vector.

It is assumed that such a consideration is well understood and therefore when a similar case occurs later in the proof it will not be analyzed.

(1) $k < u + s, u < k + s$

The following drawings are the structures of B′ and B shown in Fig. A-2.



It follows that $k = u$ and therefore $X = Y = C_1$. Referring back to Fig. A-2 we observe: $C_2Y = C_1'C_2'$. It follows that $C_1C_2 = C_2C_1$. The last equation is possible only if both C_1 and C_2 consist of a subvector A which repeats itself (i.e., $C_1 = AA \cdots A$, $C_2 = AA \cdots A$). The vector A starts with a 1 and ends with a 0, which means that it has at least two elements. Since $F_1 = C_2YDXDC_1$, it follows that $p - 2s$ is factorized. (p is the length of F_1. After deleting from it twice the vector D the rest consist of a repetition of A.)

(2) $u > k + s$

It is observed in Fig. A-2 that both C_1 and X terminate either B' or B, and they both are preceded by D. Since $u > k + s$, it follows that C_1 is terminated by DX which means that $C_1 = ZDX$.

$$B' = XDC_1 = XDZDX$$

$B = YD'X$ and therefore $Y = XDZ$

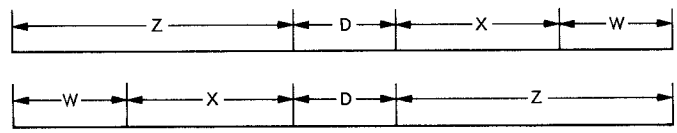
$$C_2 = C_1'W = ZDXW, C_2' = WY = WXDZ$$

and therefore

$$ZDXW = WXDZ \qquad \text{(A-3)}$$

Four different cases should be considered.

(a) In the two versions of C_2, the vector D coincides with itself.



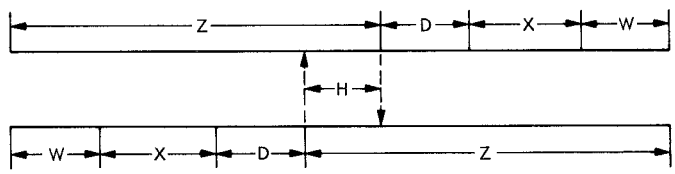
It follows that $WX = XW = Z$ and therefore W, X and Z have the form $AA \cdots A$.

$$F_1 = C_2YD'XDC_1 = ZDXWXDZDXDZDX.$$

It follows that $p - 5s$ is factorized. (After deleting D five times, the rest is a repetition of A.)

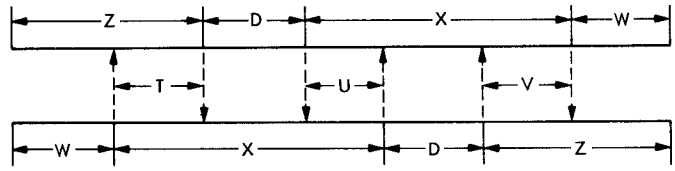
The other three cases for the possible construction of C_2 are those where D is completely contained in Z, X or W. (Any other possibility results in an immediate correspondence between the first element of any of these three vectors and an element in D.)

(b) D is completely contained in Z.



It follows that $WXDH = HDXW$ (both equal Z). Continue with Eq. (A-3).

(c) D is completely contained in X.



It follows that $TDU = UDV$ (both equal X). Continue with Eq. (A-2).

(d) D is completely contained in W.

Eq. (A-3) states that $ZDXW = WXDZ$. Suppose that D in the left side of the equation is contained in W on the right side. (This assumption is always true for D contained in W since it holds iff D on the right side of the equation is contained in W on the left side.) It follows that W has the form ZDV. Eq. (A-3) has now the form $ZDXZDV = ZDVXDZ$. It follows that $XZDV = VXDZ$. Continue with Eq. (A-1).

(3) $k > u + s$.

Both C_1 and X terminate either B' or B (as shown in Fig. A-2). It follows that X has the form ZDC_1.

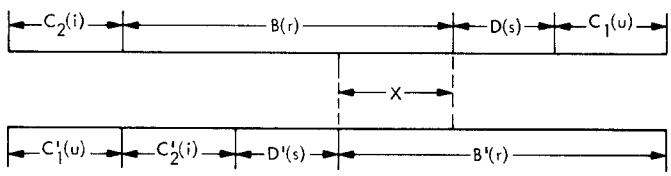
$$B' = XDC_1 = ZDC_1DC_1$$

$$B = YD'X = YDZDC_1$$

It follows that $ZDC_1 = YDZ$. Continue with Eq. (A-2).

6.2 $i = u$.

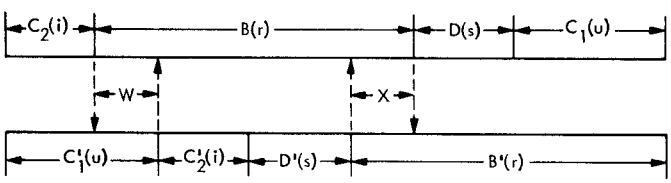
Referring to Eq. (A-1), the two arrangements of F_1 can be described as follows:



It follows that $C_1 = C_2$ and therefore $C_1DX = XDC_1$. (Both equal either B or B'.) Continue with Eq. (A-2).

6.3 $i < u$.

F_1 has the following two arrangements.



$C'_1 = C_2W$

$B' = XDC_1 = XDC_2W$

$B = WC'_2D'X$

It follows that $XDC_2W = WC_2DX$. Continue with Eq. (A-3).

The final conclusion from step 6 is that for $0 < i < t$ and $u < r$ it is possible to have $F_1 = E_1^{(i)}$ only if $p - n \cdot s$ is factorized for some n.

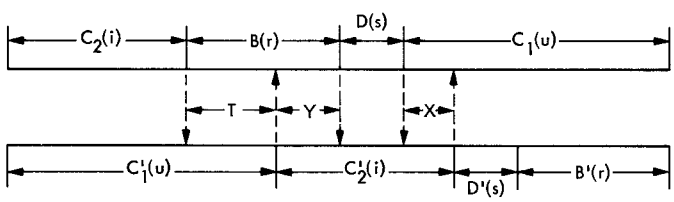
Step 7: Assume $F_1 = E_1^{(i)}, 0 < i < t, u = r$

Since $F_1 = C_2BDC_1 = C_1C_2DB$, where the length of C_1 and B is u and r, respectively, it follows that $C_1 = B$ and therefore $C_1C_2 = C_2C_1$. It follows that C_1, C_2 and B all have the form $AA \cdots A$ and $p - s$ is therefore factorized.

Step 8: Assume $F_1 = E_1^{(i)}, 0 < i < t, u > r$

8.1 $u < r + s + i$

The two arrangements of F_1 are described as follows:



$C'_1 = C_2T$

$C'_2 = YDX$

It follows that C_1 = YDXT.

$C_1 = XD'B'$

$B = TY$

It follows that $C_1 = XDTY$ and therefore

$$YDXT = XDTY \qquad \text{(A-4)}$$

Three cases are observed now.

(1) $X = Y$.

It follows that $XT = TX$ which means that Y, X and T all have the form $AA \cdots A$. $F_1 = C_2TYDXD'B' = YDXTYDXDTY$. It follows that $p - 3s$ is factorized.

(2) $Y > X$.

It follows from Eq. (A-4) that Y has the form XDV. Equation (A-4) therefore has the form

$$XDVDXT = XDTXDV.$$

It follows that $VDXT = TXDV$. Continue with Eq. (A-3).

(3) $X > Y$.

It follows from Eq. (A-4) that X has the form YDV. Equation (A-4) therefore has the form

$$YDYDVT = YDVDTY$$

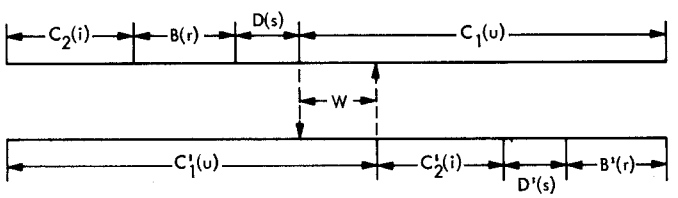
It follows that YDVT = VDTY. Continue with Eq. (A-4).

8.2 $u = r + s + i$

It follows from Eq. (A-1) that $C_2DB = C_2BD$, which means that $DB = BD$, which is impossible (1 in B corresponds to 0 in D).

8.3 $u > r + s + i$

The two arrangements of F_1 are described as follows:



It follows that $C_2BDW = WC'_2D'B'$. (Both equal either C'_1 or C_1.) Continue with Eq. (A-1).

The conclusion drawn from steps 5 to 8 is that for $0 < i < t$ it is possible to have $F_1 = E_1^{(i)}$ only if $p - n \cdot s$ is factorized for some n.

Step 9: Assume $F_1 = E_1^{(i)}$ where $i = t$

It follows that $CBD = CDB$, and therefore $DB = BD$, which is impossible since D starts with a 0 and B starts with a 1. The same applied for $i = t + s$.

Step 10: Assume $F_1 = E_1^{(i)}$ for $t < i < t + s$

$E_1 = BD_1D_2C$ where the length of D_2C is i.

$F_1 = D_2CBD_1 = CD_1D_2B$, which is impossible since F_1 starts once with a 1 and once with a 0.

Step 11: Assume $F_1 = E_1^{(i)}$ for $t + s < i$

$E_1 = B_1B_2DC$ where the length of B_2DC is i.

$F_1 = B_2DCB_1$

$F_1 = CDB_1B_2$. It follows that $B_2DCB_1 = CDB_1B_2$. Continue with Eq. (A-4).

Step 12: Conclusion of the proof of part (2) of the theorem.

It has been shown in step 3.2 and in steps 5 to 11 that if $F_1 = E_1^{(i)}$ for $p > i > 0$ then $p - n \cdot s$ is factorized for some $n \geq 0$. This means that it is sufficient to require that $p - n \cdot s$ should be primes for $n = 0,1,2, \cdots [p/]$ in order for the code to be able to correct any error burst of length $p - 1$ or less. (For values of n higher than $[p/s]$ the value of $p - n \cdot s$ is negative.)

On the other hand, for every n, $0 \leq n \leq [p/s]$ it is possible to find a vector F_1 such that $F_1 = E_1^{(i)}$ ($p > i > 0$) provided that $p - n \cdot s$ is factorized.

$$\text{For } n = \begin{Bmatrix} 0 \\ 1 \\ 2 \\ 3 \\ 5 \end{Bmatrix} \text{ the vector } F_1 \text{ is described in step} \begin{Bmatrix} 3.2 \\ 7 \\ 6.1.(1) \\ 8.1.(1) \\ 6.1(2)(a) \end{Bmatrix}$$

The following describes a systematic way by which a vector F_1 can be obtained such that $F_1 = E_1^{(i)}$ ($p > i > 0$) and $p - n \cdot s$ is factorized, for every value of n, $1 \leq n \leq [p/s]$.

If steps 5, 7 are performed, the result is that $p - s$ is factorized. If a vector V_1 whose length is d_1 is obtained by performing steps 5,8, 8.3, 7, then $d_1 - s$ is factorized. If F_1 is now reconstructed in terms of the subvectors of V_1, the result is that $p - 2s$ is factorized. Generally, if V_i is obtained by doing the steps 5, $(8,8.3)^i$, 7, then by reconstructing F_1 in terms of the subvectors of V_i the result is that $p - (i + 1) \cdot s$ is factorized.

It can be concluded that the condition stated in the theorem is sufficient and necessary, and by this part (2) of the theorem is proved.

Step 13: Proof of part (3) of the theorem

13.1 $b = p$.

It has been shown that if $F_1 = E_1^{(i)}$ for some $0 < i < p$, then $p - n \cdot s$ is factorized for some n. By this the validity of the code is proved, since it is enough to require that $p - n \cdot s$ should be prime.

The result that $p - n \cdot s$ is factorized followed from the fact that F_1 consists of n subvectors D (an "all 0" vector of length $s = q - p$), and the rest consists of repetition of a subvector A whose length is at least 2. The last result followed from the fact that $b \leq p - 1$.

If $b = p$, the repeated vector A can consist of one element. This means that it is possible to have $F_1 = E_1^{(i)}$ although $p - n \cdot s$ is prime, provided that F_1 consists of n subvectors D and $p - n \cdot s$ elements of value 1, where each pair of subvectors D is separated by at least one 1 element. It follows that F_1 — or any cyclic shift of it — do not have $q - p + 1$ successive zeroes. This means that the check for "all 0" input performed by the decoder (and demonstrated in Fig. 1.) is never satisfied. It follows that if $b = p$, the error is always detected.

13.2 $b = p + 1$

The first and last elements of the error burst are p places apart. In view of the construction of the first p rows in the parity check matrix H, it follows that if H is multiplied by the received erroneous message, the number of 1 elements in the first p places of the syndrome will be less by 2 from the corresponding number in the last q places of the syndrome, and an uncorrectable error is detected. Hardwarewise, no match is possible between the content of the first $p - 1$ stages of R_1 and R_2, where the rest of the stages contain 0. (This comment refers to Fig. 1 which describes the decoder.)

13.3 $p + 1 < b \leq q - p + 1$.

Let G be a vector of length q whose first b elements are the error pattern and the rest of its elements are 0. The last q elements of the syndrome consist of a cyclic shift of G.

Referring to the description of the decoder (Fig. 1) it is seen that in order for an error to be corrected the content of the last $q - p + 1$ stages of register R_2 is required to be all 0 in order to correct the error. The content of R_2 is a cyclic shift of G. This vector has a 1 element in its first place and bth place where $p + 1 < b \leq q - p + 1$. No cyclic shift of G can have $q - p + 1$ successive zeroes at its end. Since one of the necessary conditions for correcting the error is never met, an uncorrectable error pattern is detected.

It can be concluded from steps 13.1 to 13.3 that if $b \leq \max(p + 1, q - p + 1)$ the error is detected.

13.4 Proof of error detection probability

It is assumed here that the noise source which produces the error burst is of such a type that all transmitted information is lost during the interruption time. It is therefore assumed that the error burst has an equal probability of having any particular pattern. The probability of not detecting an error is defined as the number of undetectable patterns divided by the total number of possible patterns.

If $q - p + 1 < p + 1 < b$ or $p + 1 < q - p + 1 < b$ then for both cases the vector G (defined in section 13.3) cannot have at its end $q - p + 1$ successive zeroes. In order for a cyclic shift of it to have this number of zeroes at its end, the vector G must have $q - p + 1$ successive zeroes within the first b places. This group of zeroes can start anywhere between the second place and the $b - (q - p + 1)$ place. (The first and bth elements must be 1). These zeroes have therefore less than p different places to start with. It follows that the probability of having an undetectable error is less than $p \cdot 2^{b-2-(q-p+1)}/2^{b-2} = p \cdot 2^{p-q-1}$. The proof of the theorem is thus completed.

Table 1. Some suggested burst-correcting cyclic codes

Burst-correcting ability b	(n,k)	Rate, %	Efficiency, %	q	$p = b+1$
22	(667,616)	93.4	90.2	29	23
30	(1333,1260)	94.5	84.9	43	31
40	(2173,2080)	95.7	88.2	53	41
52	(4399,4264)	96.9	78.5	83	53
60	(6283,6120)	97.4	74.8	103	61
66	(6499,6336)	97.4	82.2	97	67
72	(7519,7344)	97.7	83.4	103	73
82	(9379,9184)	97.9	85.1	113	83
96	(12139,11916)	98.2	87	127	97
100	(13231,13000)	98.3	87.4	131	101
126	(19939,19656)	98.6	89.8	157	127
148	(29353,29008)	98.8	86.4	197	149
250	(78061,77500)	99.3	89.5	311	251

Table 2. Comparing some codes

b	n	Suggested code		"Most efficient code"		
		k	Rate, %	Original code	k	Rate, %
30	1,000	927	92.7	(121,112)	910	91
40	1,000	907	90.7	(164,153)	890	89
40	2,000	1,907	95.3	(290,277)	1,896	94.8
50	2,000	1,865	93.2	(290,277)	1,870	93.5
50	4,000	3,865	96.6	(290,277)	3,844	96.1
65	3,000	2,837	94.5	(290,277)	2,861	95.3
65	6,000	5,837	97.2	(511,499)	5,796	96.6
80	4,000	3,805	95.1	(290,277)	3,792	94.8
80	9,000	8,805	97.8	(511,499)	8,760	97.3
100	5,000	4,769	95.3	(290,277)	4,740	94.8
100	10,000	9,769	97.6	(511,499)	9,700	97